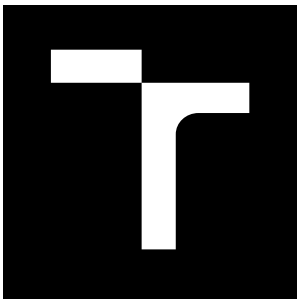

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
FACULTY OF MECHANICAL ENGINEERING

ÚSTAV MATEMATIKY
INSTITUTE OF MATHEMATICS

KVATERNIONOVÉ ALGEBRY
QUATERNION ALGEBRAS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Pavel Bečka**
AUTHOR

VEDOUCÍ PRÁCE — **doc. RNDr. Miroslav Kureš, Ph.D.**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA STROJNÍHO INŽENÝRSTVÍ

Zadání bakalářské práce

Ústav:	Ústav matematiky
Student:	**Pavel Bečka**
Studijní program:	Aplikované vědy v inženýrství
Studijní obor:	Matematické inženýrství
Vedoucí práce:	**doc. RNDr. Miroslav Kureš, Ph.D.**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma bakalářské práce:

Kvaternionové algebry

Stručná charakteristika problematiky úkolu:

Studium kvaternionových algeber, tzn. vektorových prostorů nad polem F dimenze 4 s bází 1, i, j, k, kde 1 je neutrální prvek a i2 = a, j2 = b, ij = –ji = k. Přehled základních pojmů a výsledků, samostatné příklady, výpočty s užitím softwaru.

Cíle bakalářské práce:

1) Napsat přehledný úvodní text o kvaternionových algebrách.
2) Uvést aplikace.
3) Pojmy ilustrovat četnými příklady a cvičeními (vhodné je použití open source systému počítačové algebry SAGE).
Smyslem práce je, aby se student naučil pracovat s náročnějšími algebraickými pojmy a vytvořil text s didaktickou hodnotou.

Seznam doporučené literatury:

MACLACHLAN, C. and A. W. REID. The Arithmetic of Hyperbolic 3-Manifolds. Springer. 2003. ISBN 978-0-387-98386-8.

VIGNÉRAS, M. F. Arithmétique des Algèbres de Quaternions. Lecture Notes in Mathematics. Springer. 1980. ISBN 978-3-540-09983-3.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2016/17

V Brně, dne

L. S.

prof. RNDr. Josef Šlapal, CSc. ředitel ústavu	doc. Ing. Jaroslav Katolický, Ph.D. děkan fakulty

Abstrakt
V této práci jsou rozebírané kvaternionové algebry, tedy čtyřrozměrné vektorové prostory s bází $1, i, j, k$ a zavedeným násobením $i^2 = a$, $j^2 = b$, $ij = -ji = k$. V práci se zabýváme základními vlastnostmi kvaternionových algeber. Dále pak pojmem řádu a problematikou maximálního řádu. Nakonec se zabýváme diskriminantem kvaternionových algeber a s tím spojených pojmů jako je Hilbertův symbol a Legendreův symbol. Napříč prací jsou uvedené řešené příklady za podpory matematického softwaru SAGE.

Summary
This thesis deals with quaternion algebras. A quaternion algebra is a four dimensional vector space with basis $1, i, j, k$ and multiplication defined as $i^2 = a$, $j^2 = b$, $ij = -ji = k$. The thesis deals with the basic attributes of quaternion algebras, quaternion orders and maximal orders. Lastly the thesis deals with the concept of discriminant of algebras and connected terms like Hilbert symbol and Legendre symbol. Throughout the thesis we show solved problems using mathematical software SAGE.

Klíčová slova
kvaternionová algebra, řád, maximální řád, SAGE, diskriminant kvaternionové algebry, Hilbertův symbol

Keywords
quaternion algebra, order, maximal order, SAGE, discriminant of quaternion algebra, Hilbert symbol

BEČKA, P. *Kvaternionové algebry.* Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2017. ?? s. Vedoucí doc. RNDr. Miroslav Kureš, Ph.D.

Prohlašuji, že jsem bakalářskou práci „Kvaternionové Algebry“ zpracoval samostatně pod vedením vedoucího doc. RNDr. Miroslavem Kurešem Ph.D. za využití zdrojů uvedených v seznamu použité literatury.

Pavel Bečka

Chtěl bych poděkovat zejména svému vedoucímu práce za vytrvalou odbornou pomoc. Dále pak svojí přítelkyni Zuzaně za psychickou podporu a pomoc s pravopisnou stánkou práce.

Pavel Bečka

Obsah

1 Úvod **2**

2 Definice kvaternionové algebry **3**
2.1 První definice . . . 3
2.2 Norma, stopa . . . 4
2.3 Druhá definice . . . 5
2.4 SAGE . . . 6
2.5 Příklady . . . 6

3 Řády kvaternionových algeber **9**
3.1 Definice řádu . . . 9
3.2 Maximální řád . . . 9
3.3 Výpočty řádů . . . 10

4 Diskriminant **15**
4.1 p-adická valuace . . . 15
4.2 Legendreův symbol . . . 15
4.3 Hilbertův symbol . . . 16
4.4 Diskriminant . . . 19
4.5 Výpočet diskriminantu na konkrétním příkladu . . . 19

5 Závěr **22**

6 Seznam použitých zkratek a symbolů **24**

1. Úvod

Tato práce se zabývá studiem kvaternionových algeber. Jedná se o čtyřrozměrné vektorové prostory s nekomutativním násbením. Můžeme se na ně dívat jako na čtyřrozměrnou podobu komplexních čísel.

V první kapitole se zabýváme zavedením kvaternionových algeber a jejich vlastnostmi. Jsou uvedeny dvě definice a důkaz jejich ekvivalence. Na závěr kapitoly jsou uvedeny řešené příklady.

V druhé kapitole se zabýváme problematikou řádů a maximálních řádů kvaternionových algeber, což je paralela na okruhy jednotek v číselných polích. Opět jsou uvedeny řešené příklady podpořené výpočty v programu SAGE. SAGE je matematický software, který umí počítat s algebraickými strukturami. Můžeme s jeho pomocí například počítat maximální řády kvaternionových algeber nad racionálními čísly.

V poslední kapitole je rozebrána problematika diskriminantu algeber, podrobněji pak pro kvaternionové algebry. Na závěr je uveden výpočet diskriminantu pro kvaternionové algebry typu $\left(\frac{-1,b}{\mathbb{Q}}\right)$, kde $b \in \mathbb{Z}$

2. Definice kvaternionové algebry

2.1. První definice

Definice 1. *R-algebra* A je okruh s jedničkou s okruhovým homomorfismem $f : R \to A$, kde platí $f(1_R) = 1_A$ a $f(R) \subseteq Z(A)$.

Definice 2. Řekneme, že A je *kvaternionová algebra* nad polem F ($char(F) \neq 2$), když A je čtyřrozměrný vektorový prostor nad F s bází $\{1, i, j, k\}$, 1 je neutrální prvek vzhledem k násobení v F a platí:

$$i^2 = a, \quad j^2 = b, \quad ij = -ji = k,$$

kde $a, b \in F^*$. Kde F^* je multiplikativní grupa nenulových prvků v F.
Kvaternionovou algebru můžeme zapsat pomocí Hilbertova symbolu:

$$\left(\frac{a,b}{F}\right).$$

Pro jakékoli pole F platí:

$$M_2(F) \cong \left(\frac{1,1}{F}\right).$$

Isomorfismus snadno dostaneme následujícím způsobem zobrazením φ:

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Věta 1.

$$\left(\frac{a,b}{F}\right) \cong \left(\frac{ax^2, by^2}{F}\right) \quad \text{Pro } \forall \mathrm{a, b, x, y} \in \overline{\mathrm{F}}.$$

Důkaz. Mějme $A = \left(\frac{a,b}{F}\right)$ s bází $\{1, i, j, k\}$ a $A' = \left(\frac{ax^2,by^2}{F}\right)$ s bází $\{1, i', j', k'\}$.

Vezmeme $\phi : A' \to A = \begin{cases} \phi(1) = 1 \\ \phi(i') = xi \\ \phi(j') = xj \\ \phi(k') = xyij \end{cases}$

Pro ověření, zda se jedná o isomorfismus musíme zkontrolovat zda $\phi(ab) = \phi(a) \cdot \phi(b)$ pro $\forall a, b \in F$.
$x^2a = xixi = \phi(i')\phi(i') = \phi(i'^2) = \phi(x^2a) = x^2a\phi(1) = x^2a$
Obdobně pro ostatní kombinace $1, i, j, k$. Dostáváme tak isomorfismus ϕ. □

Poznámka: Nemá tedy smysl zabývat se případy, kdy a, či b má v prvočíselném rozkladu druhou, či vyšší mocninu nějakého prvočísla. Budeme tedy uvažovat pouze případy kdy je a, b „square-free“.

Pro zavedení pojmu normy a stopy algebry a druhé definice kvaternionových algeber budeme potřebovat několik dalších pojmů.

Definice 3. *Centrum okruhu* R je definováno jako $Z(R) = \{a \in R | ra = ar, \forall r \in R\}$.

Definice 4. R-algebra je *centrální*, jestliže $f(R) = Z(A)$.

Definice 5. A je *jednoduchá R-algebra*, jestliže má pouze triviální oboustranné idály.

Věta 2. Centrem kvaternionové algebry $A = (\frac{a,b}{F})$ je F. Tedy A je centrální.

Důkaz. $(\frac{a,b}{F}) \otimes_F \overline{F} = (\frac{a,b}{\overline{F}})$. V $\overline{F}$ je každý prvek druhou mocninou jiného prvku, tedy $(\frac{a,b}{\overline{F}}) \cong (\frac{1,1}{\overline{F}}) \cong M_2(\overline{F})$. $Z\left(M_2(\overline{F})\right) = \overline{F}$. Tedy dostáváme $Z(A) = F$. □

Věta 3. *$A = (\frac{a,b}{F})$ je jednoduchá F-algebra.*

Důkaz. Mějme nenulový ideál $I \subseteq A$. $\overline{F}$ je algebraický uzávěr pole F. Protože $(\frac{a,b}{F}) \otimes_F \overline{F} = (\frac{a,b}{\overline{F}})$, musí platit $I \otimes_F \overline{F}$ je nenulový ideál v $M_2(\overline{F})$.
$M_2(\overline{F})$ je jednoduchá algebra a $dim(F) = 4$ a dostáváme tedy pouze $I = A$, triviální ideál. □

Definice 6. Mějme A komutativní algebru nad F. A nazveme *separabilní*, pokud $A \cong F[x]/(f(x))$, kde $f(x)$ je polynom s různými kořeny v $\overline{F}$.

2.2. Norma, stopa

V této části se budeme zabývat normou a stopou kvaternionových algeber. Pro začátek však budeme potřebovat několik dalších pojmů.

Definice 7. Nechť A_0 je podprostor A generovaný vektory i, j, k. Pak $a \in A_0$ nazveme *čistý kvaternion.*

Věta 4. $x \in A - \{0\}$ je čistý kvaternion právě tehdy když $x \notin Z(A) \wedge x^2 \in Z(A)$.

Důkaz. Mějme $x = a_0 + a_1 i + a_2 j + a_3 k$, pak

$$x^2 = (a_0^2 + a_1^2 + a_2^2 + a_3^2) + 2a_0(a_1 i + a_2 j + a_3 k). \tag{2.1}$$

($\Rightarrow$) x je čistý kvaternion tedy $x = a_1 i + a_2 j + a_3 k$. Je zřejmé, že $x \notin Z(A)$. Z (**??**) vidíme, že když platí $a_0 = 0$, tak $x^2 \in Z(A)$.
($\Leftarrow$) Z (**??**) vidíme, že $a_0 = 0$, aby platilo $x \in Z(A)$. Tedy x je tvořen lineární kombiací $\{i, j, k\}$, tedy x je čistý kvaternion. □

Každý prvek $x \in A$ tedy můžeme zapsat jako $x = a + \alpha$ kde $a \in Z(A)$, $\alpha \in A_0$.

Definice 8. Nechť $x \in A$. x můžeme zapsat jako $x = a + \alpha$ kde $a \in Z(A)$, $\alpha \in A_0$. Pak definujeme *konjugaci* jako $\overline{x} = a - \alpha$

Definice 9. Pro $x \in A$ definujeme *normu*:

$$n(x) = x\overline{x}$$

a *stopu*:

$$tr(x) = x + \overline{x}.$$

Tedy když $x \in \left(\frac{a,b}{F}\right)$ zapíšeme jako $x = a_0 + a_1 i + a_2 j + a_3 k$, kde $a_i \in F$ pro normu a stopu platí:

$$n(x) = a_0^2 - aa_1^2 - ba_2^2 + aba_3^2,$$
$$tr(x) = 2a_0.$$

Pro normu n platí: $n(xy) = (xy)\overline{(xy)} = x\,y\,\overline{y}\,\overline{x} = n(x)n(y)$. Tedy invertovatelné prvky jsou ty pro které platí $x \neq 0$.

$$x^{-1} = \frac{\overline{x}}{n(x)}$$

V případě Hamiltonových kvaternionů $\mathcal{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ platí pro normu $n(x) = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Tedy každý prvek je invertovatelný, tedy $\mathcal{H}$ je algebra s dělením.
Kvaternionové algebry, které jsou isomorfní s $M_2(F)$ samozřejmě nejsou algebrami s dělením.

Věta 5. Platí:

$$tr(x^2) = tr(x)^2 - 2n(x).$$

Důkaz. Důkaz získáme přímým dosazením za $tr(x)$ a $n(x)$.

$$\begin{aligned} tr(x^2) &= tr(x)^2 - 2n(x) \\ x^2 + \overline{x}^2 &= (x + \overline{x})^2 - 2x\overline{x} \\ x^2 + \overline{x}^2 &= x^2 + 2x\overline{x} + 2\overline{x}^2 - 2x\overline{x} \end{aligned}$$

□

2.3. Druhá definice

Definice 10. Máme pole F. A je čtyřrozměrná centrální algebra nad F s centrem F tak, že existuje separabilní algebra L dimenze 2 nad F tak, že $A = L + Lu$, kde $u \in A$ splňuje:

$$u^2 = \Theta, \quad um = \overline{m}u, \quad \Theta \in F^*.$$

Pak řekneme, že A je *kvaternionová algebra*.

Věta 6. Definice **??** a definice **??** jsou ekvivalentní.

Důkaz. Mějme kvaternionovou algebru podle definice **??**. L je separabilní algebra dimenze 2. Má tedy své generátory. Označme je $1, y$. Nyní vezmeme kvaternionovou algebru podle definice **??**. a vezmeme bázi $\{1, y, u, yu\}$.
Vezměme kvaternionovou algebru podle definice **??** s bází $\{1, i, j, k\}$. Tato algebra je centrální a jednoduchá. $F(i)$ je separabilní. Vezmeme tedy $L = F(i)$ a $u = j$. Stačí pak ověřit podmínky definice **??**.

$$um = \overline{m}u,$$

$m \in L$ jsou tvaru $m = a_0 + a_1 i, \quad u = j$.

$$um = j(a_0 + a_1 i) = a_0 j + a_1 ji = a_0 j - a_1 ij = (a_0 - a_1 i)\, j = \overline{m}u$$

□

2.4. SAGE

V této práci je použit k výpočtům software SAGE. Je volně dostupný na stránkách www.sagemath.org. Existuje webové rozhraní, nebo lze stáhnout zdrojový kód pod GPL licencí. Tedy zdrojový kód je volně k dispozici k nastudování i k úpravě.
Pro účely této práce bylo využito webového rozhraní fungujícího na neplacených serverech.
Na následujícím příkladu je ilustrováno, jak budou v práci zapisovány příklady v SAGE. Všechny příkazy budou začínat „SAGE:“.

```
SAGE: 10+5*8+6/9
152/3
```

Abychom vytvořili kvaternionovou algebru A použijeme následující příkaz.

```
SAGE: A.<i, j, k> = QuaternionAlgebra(QQ, a, b)
```

Kde $a = i^2$, $b = j^2$, QQ značí obor racionálních čísel $\mathbb{Q}$.
V dalších příkazech pak tedy můžeme používat i, j, k v smyslu dané kvaternionové algebry. Pokud nepotřebujeme počítat s jednotlivými prvky, ale budeme po SAGE chtít jen obecné vlastnosti algebry stačí:

```
SAGE: A=QuaternionAlgebra(QQ, a, b)
```

2.5. Příklady

Příklad 1. Nejznámějším příkladem jsou *Hamiltonovy kvaterniony*. $\mathcal{H} = (\frac{-1,-1}{\mathbb{R}})$. Připomeňme, že jsou definovány pomocí

$$i^2 = j^2 = k^2 = -1$$

a pro součin dvou libovolných prvků platí:

$$(a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k) =$$

$$= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)\, i +$$
$$+ (a_1 c_2 + c_1 a_2 - b_1 d_2 + s_1 b_2)\, j + (a_1 d_2 + d_1 a_2 + b_1 c_2 - c_1 b_2)\, k,$$

kde $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{R}$.

Příklad 2. Jako jiný příklad vezměme $A = (\frac{-5,-10}{\mathbb{Q}})$ a dva prvky $x, y \in A$. Spočtěme jejich součin.

$$x = 1 + i + j + k$$

$$y = 2 + 2i + 2j + 2k$$

$$\begin{aligned} x \cdot y &= (1 + i + j + k) \cdot (2 + 2i + 2j + 2k) = \\ &= (2 + 2i + 2j + 2k) + (2i + 2i^2 + 2ij + 2ik) + (2j + 2ji + 2j^2 + 2jk) + \\ &\quad + (2k + 2ki + 2kj + 2k^2) = \\ &= (2 + 2i + 2j + 2k) + (2i - 10 + 2k - 10j) + (2j - 2k - 20 + 20i) + \\ &\quad + (2k + 10j - 20i - 100) = \\ &- 128 + 4i + 4j + 4k \end{aligned}$$

Výsledek můžeme snadno ověřit v programu SAGE.

SAGE: A.$\langle i, j, k \rangle$ = QuaternionAlgebra(QQ, $-5, -10$)
SAGE :(1 + i + j + k) $*$ (2 + 2 $*$ i + 2 $*$ j + 2 $*$ k)
-128 + 4*i + 4*j + 4*k

Příklad 3. Ukažte, že

$$A = \left\{ \begin{pmatrix} \alpha & 5\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix} \mid \quad \alpha, \beta \in \mathbb{Q}(\sqrt{-3}) \right\}$$

je kvaternionová algebra nad $\mathbb{Q}$ a $A \cong \left(\frac{-3,5}{\mathbb{Q}}\right)$.
Řešení: A můžeme zapsat následujícím způsobem:

$$A = \left\{ a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} \sqrt{-3} & 0 \\ 0 & \sqrt{-3} \end{pmatrix} + c \begin{pmatrix} 0 & 5 \\ 1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & 5\sqrt{-3} \\ \sqrt{-3} & 0 \end{pmatrix} \mid \quad a, b, c, d \in \mathbb{Q} \right\}.$$

Vezmeme zobrazení $\varphi : A \to \left(\frac{-3,5}{\mathbb{Q}}\right)$

$1_A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \to 1,$

$i_A = \begin{pmatrix} \sqrt{-3} & 0 \\ 0 & -\sqrt{-3} \end{pmatrix} \to i,$

$j_A = \begin{pmatrix} 0 & 5 \\ 1 & 0 \end{pmatrix} \to j,$

$k_A = \begin{pmatrix} 0 & 5\sqrt{-3} \\ -\sqrt{-3} & 0 \end{pmatrix} \to k.$

Musíme ověřit zda je φ homomorfismem. Je třeba ověřit zda platí $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ pro $a, b \in A$. Tuto podmínku stačí ověřit pro všechny kombinace bázových vektorů. Kvůli zdlouhavosti je uveden pouze ilustrační příklad pro $\varphi(i_A \cdot i_A)$ a $\varphi(j_A \cdot k_A)$.

$\varphi(i_A \cdot i_A) = \varphi\left(\begin{pmatrix} \sqrt{-3} & 0 \\ 0 & -\sqrt{-3} \end{pmatrix} \cdot \begin{pmatrix} \sqrt{-3} & 0 \\ 0 & -\sqrt{-3} \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} -3 & 0 \\ 0 & -3 \end{pmatrix}\right) = -3 = i^2 =$
$= \varphi(i_A)\varphi(i_A)$

$\varphi(j_A \cdot k_A) = \varphi\left(\begin{pmatrix} 0 & 5 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 5\sqrt{-3} \\ -\sqrt{-3} & 0 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} -5\sqrt{-3} & 0 \\ 0 & 5\sqrt{-3} \end{pmatrix}\right) = -5i = -j^2 i =$
$= -jji = jij = jk = \varphi(j_A) \cdot \varphi(k_A)$

Příklad 4. Ukažte, že Hamiltonovy kvaterniony jsou isomorfní k podalgebře matic druhého řádu v komplexních číslech. $\mathcal{H} = \left(\frac{-1,-1}{\mathbb{R}}\right) \cong \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\} = B.$

Vezměme standardní bázi $\mathcal{H}$ a oynačme ji následujícím způsobem: $\{1_\mathcal{H}, i_\mathcal{H}, j_\mathcal{H}, k_\mathcal{H}\}$. Nyní vezmeme zobrazení $\varphi : \mathcal{H} \to B$ a dokážeme, že je isomorfismem.
$1_\mathcal{H} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i_\mathcal{H} \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j_\mathcal{H} \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k_\mathcal{H} \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$
Neboli $a_0 + a_1 i_\mathcal{H} + a_2 j_\mathcal{H} + a_3 k_\mathcal{H} \mapsto \begin{pmatrix} a_0 + a_1 & a_2 + a_3 \\ -a_2 + a_3 & a_0 - a_1 \end{pmatrix}$, kde $a_0, a_1, a_2, a_3 \in \mathbb{R}$.

Pro dokázání, že se jedná o isomorfismus stačí dokázat, že φ zachovává operaci pro všechny kombinace násobení bázových vektorů v $\mathcal{H}$.
$\varphi(i_\mathcal{H} \cdot i_\mathcal{H}) = \varphi(-1_\mathcal{H}) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$\varphi(i_\mathcal{H}) \cdot \varphi(i_\mathcal{H}) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$\varphi(i_\mathcal{H} \cdot j_\mathcal{H}) = \varphi(k_\mathcal{H}) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$
$\varphi(i_\mathcal{H}) \cdot \varphi(j_\mathcal{H}) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$
$\varphi(i_\mathcal{H} \cdot k_\mathcal{H}) = \varphi(-j_\mathcal{H}) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
$\varphi(i_\mathcal{H}) \cdot \varphi(k_\mathcal{H}) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
$\varphi(j_\mathcal{H} \cdot j_\mathcal{H}) = \varphi(-1_\mathcal{H}) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$\varphi(j_\mathcal{H}) \cdot \varphi(j_\mathcal{H}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$\varphi(j_\mathcal{H} \cdot k_\mathcal{H}) = \varphi(i_\mathcal{H}) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$
$\varphi(j_\mathcal{H}) \cdot \varphi(k_\mathcal{H}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$
$\varphi(k_\mathcal{H} \cdot k_\mathcal{H}) = \varphi(-1_\mathcal{H}) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$\varphi(k_\mathcal{H}) \cdot \varphi(k_\mathcal{H}) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
Kombinace s $1_\mathcal{H}$ jsou zřejmě platné, protože $1_\mathcal{H}$ se zobrazuje na jednotkovou matici. Proto je zde neuvádíme.

3. Řády kvaternionových algeber

3.1. Definice řádu

Definice 11. Nechť V je vektorový rostor nad F, *R-mřížka* L je konečně generovaný R-modul ve V. Dále pokud platí $L \otimes_R F \cong V$, L nazveme *úplnou R-mřížkou*.

Věta 7. Mějme kvaternionovou algebru $A = \left(\frac{a,b}{F}\right)$. Pak prvek $\alpha \in A$ je *jednotka* nad R pokud $R[\alpha]$ je R-mřížka v A.

Definice 12. *Ideál* I v algebře A je úplná R-mřížka.

Definice 13. *Řád* O v A je ideál I, který je zároveň okruh s jedničkou.

Definice 14. Řád O je *maximální řád* pokud je maximální vzhledem k inkluzi.

3.2. Maximální řád

V programu SAGE jsou funkce pro kontrolu a výpočet řádů a maximálních řádů naprogramovány pouze pro okruh racionálních čísel, proto se jimi budeme zabývat podrobněji. Pro kontrolu, zda je daná množina okruh můžeme použít příkaz *quaternion_order()*. Nejprve vezmeme řád se standardní bází $\{1, i, j, k\}$, poté $\{1, 2i, 2j, 2k\}$.

```
SAGE: A=QuaternionAlgebra(QQ,-1,-2)
SAGE: Q=A.quaternion_order([1,i,j,k])
SAGE: Q
Order of Quaternion Algebra (-1, -2) with base ring Rational Field with basis (1, i,
j, k)
SAGE: R=A.quaternion_order([1,2*i,2*j,2*k])
SAGE: R
Order of Quaternion Algebra (-1, -2) with base ring Rational Field with basis (1,
2*i, 2*j, 2*k)
```

SAGE umí počítat i maximální řády, ale znovu pouze v racionálních číslech. V minulosti uměl počítat maximální řády jen pro kvaternionové algebry s prvočíselným diskriminantem. [?Macalkova$_S AGE$?]$Nynvesvmalgoritmuvyuvdliteldiskriminantu.Pojmemdiskriminantseb$

```
SAGE: A=QuaternionAlgebra(QQ,-10,30)
SAGE: A.discriminant()
15
SAGE: A.maximal_order()
Order of Quaternion Algebra (-10, 30) with base ring Rational Field with basis (1,
i, 1/2 + 1/4*i + 1/4*j, 1/2 + 1/2*i + 1/20*k)
```

Pro speciální případy kvaternionových algeber algoritmus přiřazuje konkrétní maximální řády.[1] Například pro kvaternionovou algebru $A = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ algoritmus přiřadí maxi-

[1] V adresáři zdrojového kódu je kód pro práci s kvaternionovými algebrami v souboru src*sage\agebras\quatalg\quaternion_algebra.py*

mální řád s bází $\left\{\frac{1}{2}+\frac{1}{2}i+\frac{1}{2}j+\frac{1}{2}k, i, j, k\right\}$. Tento řád se nazývá Hurwitzovy kvaterniony. Pokud není algebra jedním ze speciálních případů, proběhne algoritmus samotný. Vezmeme řád se standardní bází. Spočteme diskriminant A. Pak pro každého dělitele diskriminantu zvětšujeme řád. Diskriminantem kvaternionových algeber se budeme zabývat v Kapitole **??**.

3.3. Výpočty řádů

V této části práce uvedeme několik řešených příkladů na téma řádů a maximálních řádů kvaternionových algeber.

Příklad 5. Ukažte, že. $\mathcal{O} = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid a \equiv d \,(mod\, 2),\ b \equiv c \,(mod\, 2)\right\}$ je řád v $M_2(\mathbb{Q})$.
Musíme dokázat, že $\mathcal{O}$ je *ideál* (úplná R-mřížkou) a okruh s jedničkou.
Je zřejmé, že $\mathcal{O}$ je úplnou R-mřížkou. $\mathcal{O}$ můžeme zapsat jako:
$\mathcal{O} = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c = 2n + (b \,mod\, 2), d = 2m + (a \,mod\, 2), \quad a, b, n, m \in \mathbb{Z}\right\}$
Musíme tedy dokázat, že $\mathcal{O}$ je okruhem s jedničkou.
Vezměme dva prvky $A, B \in \mathcal{O}$. $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Pak musí platit $A + B \in \mathcal{O}$.

$$A + B = \begin{pmatrix} a+\alpha & b+\beta \\ c+\gamma & d+\delta \end{pmatrix},$$

$a \equiv d \wedge \alpha \equiv \delta \pmod 2 \Rightarrow \quad a + \alpha \equiv d + \delta \pmod 2$,
$b \equiv c \wedge \beta \equiv \gamma \pmod 2 \Rightarrow \quad b + \beta \equiv c + \gamma \pmod 2$.
Tedy $\mathcal{O}$ je uzavřená vůči sčítání. Dále musí platit $AB \in \mathcal{O}$.

$$A \cdot B = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + a\gamma & c\beta + d\delta \end{pmatrix}.$$

Musíme dokázat, že $A \cdot B \in \mathcal{O}$, tedy že platí
$a\alpha + b\gamma \equiv c\beta + d\delta \pmod 2$,
$a\beta + b\delta \equiv c\alpha + d\gamma \pmod 2$.

1. $a = 2n_a \Rightarrow d = 2n_d$
   - $b = 2n_b \Rightarrow c = 2n_c$

$$\begin{aligned} a\alpha + b\gamma &\equiv c\beta + d\delta \quad (mod\, 2) \\ 2n_a\alpha + 2n_b\gamma &\equiv 2n_c\beta + 2n_d\delta \quad (mod\, 2) \\ 2(n_a\alpha + n_b\gamma) &\equiv 2(n_c\beta + n_d\delta) \quad (mod\, 2) \end{aligned}$$

   - $b = 2n_b + 1 \Rightarrow c = 2n_c + 1$

$$\begin{aligned} 2n_a\alpha + 2n_b\gamma + \gamma &\equiv 2n_c\beta + \beta + 2n_d\delta \quad (mod\, 2) \\ \gamma &\equiv \beta \quad (mod\, 2) \end{aligned}$$

2. $a = 2n_a + 1 \Rightarrow d = 2n_d + 1$

   - $b = 2n_b \Rightarrow c = 2n_c$

$$2n_a\alpha + \alpha + 2n_b\gamma \equiv 2n_c\beta + 2n_d\delta + \delta \pmod 2$$
$$\alpha \equiv \delta \pmod 2$$

   - $b = 2n_b + 1 \Rightarrow c = 2n_c + 1$

$$2n_a\alpha + \alpha + 2n_b\gamma + \gamma \equiv 2n_c\beta + \beta + 2n_d\delta + \delta \pmod 2$$
$$\alpha + \gamma \equiv \beta + \delta \pmod 2$$

Podmínku $a\beta + b\delta \equiv c\alpha + d\gamma \pmod 2$ lze ověřit úplně stejně.
Nakonec nám zbývá zjistit, zda je $\mathcal{O}$ obsahuje jedničku. $1_{M_2(Q)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Je zřejmé, že platí $1 \equiv 1 \pmod 2$ a $0 \equiv 0 \pmod 2$.

Příklad 6. Zkusme vypočítat maximální řád algebry $\left(\frac{-1,b}{\mathbb{Q}}\right)$ kde $b \in \mathbb{Z}$.
Kdybychom vzali řád obecnou bází

$$\mathcal{O} = \left\{ \alpha\left(\frac{a_1}{A_1} + \frac{b_1}{B_1}i + \frac{c_1}{C_1}j + \frac{d_1}{D_1}k\right) + \beta\left(\frac{a_2}{A_2} + \frac{b_2}{B_2}i + \frac{c_2}{C_2}j + \frac{d_2}{D_2}k\right) + \right.$$
$$\left. + \gamma\left(\frac{a_3}{A_3} + \frac{b_3}{B_3}i + \frac{c_3}{C_3}j + \frac{d_3}{D_3}k\right) + \delta\left(\frac{a_4}{A_4} + \frac{b_4}{B_4}i + \frac{c_4}{C_4}j + \frac{d_4}{D_4}k\right) \right\}.$$

Roznásobením dvou libovolných prvků a následnou kontrolou, zda je výsledek stále v množině $\mathcal{O}$ dostaneme pouze 4 rovnice o 36 neznámých. 4 neznámé pro koeficienty u báze pro výsledek násobení a 32 pro bázi samotnou. Nabízí se zde několik možností. Nebrat koeficienty v bázi samotné jako zlomky a tím snížit počet neznámých o 16. Tímto krokem sice snížíme počet neznámých, ale pořád bude soustava neřešitelná a navíc ji budeme muset řešit v racionálních číslech a ne celých. Další možnost je některé členy určit pevně. Tím ale ztratíme úplnou obecnost a nezjistíme, zda se jedná o maximální řád a inspirovat se v jakém tvaru hledat bázi.
Pomocí SAGE můžeme nechat vypsat maximální řády pro různá b.

```
SAGE: for d in ( m for m in range(-22, 0) if is_squarefree(m) ):
SAGE:     A = QuaternionAlgebra(-1,d)
SAGE:     print A.maximal_order()

Order of Quaternion Algebra (-1, -22) with base ring Rational Field with basis
(1, i, 1/2 + 1/2*i + 1/2*j, 1/2 + 1/4*j + 1/4*k)
Order of Quaternion Algebra (-1, -21) with base ring Rational Field with basis
(1, i, j, 1/2 + 1/2*i + 1/2*j + 1/2*k)
Order of Quaternion Algebra (-1, -19) with base ring Rational Field with basis
(1/2 + 1/2*j, 1/2*i + 1/2*k, j, k)
Order of Quaternion Algebra (-1, -17) with base ring Rational Field with basis
(1, i, j, 1/2 + 1/2*i + 13/34*j + 1/34*k)
Order of Quaternion Algebra (-1, -15) with base ring Rational Field with basis
(1, i, 1/2*i + 1/2*j, 1/2 + 1/2*i + 3/10*j + 1/10*k)
Order of Quaternion Algebra (-1, -14) with base ring Rational Field with basis
(1, i, 1/2 + 1/2*i + 1/2*j, 1/2 + 1/4*j + 1/4*k)
Order of Quaternion Algebra (-1, -13) with base ring Rational Field with basis
(1, i, j, 1/2 + 1/2*i + 21/26*j + 1/26*k)
Order of Quaternion Algebra (-1, -11) with base ring Rational Field with basis
(1/2 + 1/2*j, 1/2*i + 1/2*k, j, k)
Order of Quaternion Algebra (-1, -10) with base ring Rational Field with basis
(1, i, 1/2 + 1/2*i + 1/2*j, 3/10*j + 1/10*k)
Order of Quaternion Algebra (-1, -7) with base ring Rational Field with basis
(1/2 + 1/2*j, 1/2*i + 1/2*k, j, k)
Order of Quaternion Algebra (-1, -6) with base ring Rational Field with basis
(1, i, 1/2 + 1/2*i + 1/2*j, 1/2 + 1/4*j + 1/4*k)
Order of Quaternion Algebra (-1, -5) with base ring Rational Field with basis
(1, i, j, 1/2 + 1/2*i + 3/10*j + 1/10*k)
Order of Quaternion Algebra (-1, -3) with base ring Rational Field with basis
(1/2 + 1/2*j, 1/2*i + 1/2*k, j, k)
Order of Quaternion Algebra (-1, -2) with base ring Rational Field with basis
(1, i, 1/2 + 1/2*i + 1/2*j, 1/2 + 1/2*i + 1/2*k)
Order of Quaternion Algebra (-1, -1) with base ring Rational Field with basis
(1/2 + 1/2*i + 1/2*j + 1/2*k, i, j, k)
```

Můžeme si všimnout, že některé maximální řády mají bázi $\left\{1, i, j, \frac{1}{2} + \frac{1}{2}i + cj + dk\right\}$, kde $c, d \in \mathbb{Q}$ jsou funkcí b. Označme množinu tvořenou touto bází O.
Znovu musí platit, že součin jakékoli kombinace 2 prvků báze musí padnout do množiny O. Násobení 1 je zřejmě v O. Kvaternionové algebry jsou sice nekomutativní, ale stačí zkontrolovat pouze jednu dvojici, protože by pouze některé členy vyšly s opačným znamínkem a to nemá vliv na celočíslenost, kterou kontrolujeme.
$ij = k = \frac{1}{d}(\frac{1}{2} + \frac{i}{2} + cj + dk) - \frac{1}{2d} - \frac{i}{2d} - \frac{c}{d}j,$
$i(\frac{1}{2} + \frac{1}{2}i + cj + dk) = \frac{i}{2} - \frac{1}{2} + ck - dj = \frac{c}{d}(\frac{1}{2} + \frac{i}{2} + cj + dk) - \frac{c}{2d} - \frac{c}{2d}i - \frac{c^2}{d}j + \frac{i}{2} - \frac{1}{2} - dj,$
$j(\frac{1}{2} + \frac{1}{2}i + cj + dk) = \frac{j}{2} - \frac{k}{2} + cb - dbi = -\frac{1}{2d}(\frac{1}{2} + \frac{1}{2}i + cj + dk) + \frac{1}{4d} + \frac{i}{4d} + \frac{c}{2d}j + \frac{1}{2}j - dbi + cb,$
$(\frac{1}{2} + \frac{1}{2}i + cj + dk)(\frac{1}{2} + \frac{1}{2}i + cj + dk) = (\frac{1}{2} + \frac{1}{2}i + cj + dk) - \frac{1}{2} + c^2b + d^2b.$

Dostáváme tak podmínky:

1. $\frac{1}{d} \in \mathbb{Z}$
2. $\frac{1}{2d} \in \mathbb{Z}$
3. $\frac{c}{d} \in \mathbb{Z}$
4. $\frac{c}{2d} - \frac{1}{2} \in \mathbb{Z}$
5. $\frac{c^2}{d} + d \in \mathbb{Z}$
6. $\frac{1}{2d} \in \mathbb{Z}$
7. $cb + \frac{1}{4d} \in \mathbb{Z}$
8. $\frac{1}{4d} - db \in \mathbb{Z}$
9. $\frac{1}{2} + \frac{c}{2d} \in \mathbb{Z}$

Z podmínky 1., 2. máme $\frac{1}{2d} \in \mathbb{Z}$. Zksme vzít $d = \frac{1}{gb}$, kde $g \in \mathbb{Z}$.
Dosadíme do podmínky 8.:

$$\frac{1}{4d} - db = \frac{gb}{4} - \frac{1}{g} = \frac{g^2b - 4}{4g}.$$

Hledáme pro které $g \in \mathbb{Z}$ padne tento výraz do $\mathbb{Z}$. Pro $g = 1$ dostaneme $\frac{b-4}{4}$ tedy $b = 0 \pmod 4$, cože není případ, kdy je b square-free.
Pro $g = 2$ dostaneme $\frac{4b-4}{4\cdot 2} = \frac{b-1}{2}$ Tedy b je liché číslo, což je splnitelná podmínka.
Pro vyšší $g = 3, 4, ..$ nemá výraz celočíselný výsledek pro jakékoli $b \in \mathbb{Z}$.
Nyní vezměme $c = c'd$ a zkontrolujme jednotlivé podmínky. Některé z nich jsou redundantní, proto jsou vynechány.
3. $\frac{c}{d} = \frac{c'd}{d} = c'$ Tedy $c' \in \mathbb{Z}$.
4. $\frac{c}{2d} - \frac{1}{2} = \frac{c'd}{2d} - \frac{1}{2} = \frac{c}{2} - \frac{1}{2}$ Tedy c' je liché.
5. $\frac{c^2}{d} + d = \frac{c'^2d^2}{d} + d = \frac{c^2+1}{2b}$.
7. $cb + \frac{1}{4d} = c'db + \frac{1}{4d} = \frac{c'b}{2b} + \frac{2b}{4} = \frac{c'}{2} + \frac{b}{2}$ Tedy c' i b jsou liché tedy podmínka je platná.
9. $\frac{1}{2} + \frac{c}{2d} = \frac{1}{2} + \frac{c'}{2}$ Což nám zase říká, že c' je liché.
Máme tedy jen jednu rovnici pro c'.

$$\frac{c^2 + 1}{2b} \in \mathbb{N}. \tag{3.1}$$

Hledáme tak c' pro které tato rovnice platí. Najdeme tak řád
$\mathcal{O} = \left\{\alpha + \beta i + \gamma j + \delta\left(\frac{1}{2} + \frac{1}{2}j + \frac{c'}{2b}j + \frac{1}{2b}k\right) \mid \alpha, \beta, \gamma, \delta \in \mathbb{Z}\right\}$,
kde b je liché a c' splňuje **??**.

4. Diskriminant

V této kapitole se budeme zabývat již dříve zmíněným pojemem *diskriminantu* algebry. Pro jeho zavedení budeme potřebovat porozumět *p-adické valuaci a metrice*, Hilbertův symbol a Legendreův symbol.

4.1. p-adická valuace

Definice 15. Nechť $n \in \mathbb{Z}$ a $p \in \mathbb{P}$. *p-adickou valuací* v n rozumíme největší $a \in \mathbb{Z}$ tak, že platí $p^a \mid n$. p-adickou valuaci v n zapisujeme $v_p(n)$.
Pro racionální číslo $b = \frac{m}{n}$ vezmeme $v_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n)$, kde $m \in \mathbb{Z}$, $n \in \mathbb{N}$.

Definice 16. Mějme $p \in \mathbb{P}$ a $a \in \mathbb{Q}$. Definujeme *p-adickou normu* $|r|_p$ následujícím způsobem:

$$|r|_p = \begin{cases} p^{-v_p(n)} & \text{pro } r \neq 0 \\ 0 & \text{pro } r = 0 \end{cases}$$

Definice 17. Dále definujeme *p-adickou metriku* na racionálních číslech standardním způsobem.

$$\rho_p(a, b) = |a - b|_p.$$

Kde $a, b \in \mathbb{Q}$, $p \in \mathbb{P}$.

Nyní můžeme zúplnit racionální čísla pomocí této metriky. Tedy každá cauchyovská posloupnost bude mít svou limitu vůči dané p-adické metrice. Dostáváme tak *p-adická čísla*. Značíme je $\mathbb{Q}_p$. $\mathbb{Q}_p$ spolu se sčítáním a násobením tvoří pole.[?Preszler?]
Mějme pole F, valuaci v, pak zúplnění F podle valuace v budeme označovat F_v.

4.2. Legendreův symbol

Legendreův symbol budeme potřebovat pro počítání Hilbertova symbolu nad racionálními čísly.
Abychom mohli zavést pojem Legendreova symbolu, musíme napřed zavést pojem *kvadratického zbytku*.

Definice 18. Řekneme, že $q \in \mathbb{N}$ je *kvadratický zbytek* modulo p pokud existuje $x \in \mathbb{Z}$ tak, že platí:

$$x^2 \equiv q \pmod{p}.$$

Definice 19. Pro $p \in \mathbb{P}$ a $a \in \mathbb{Z}$ zavádáme *Legendreův symbol* jako:

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{pokud a je kvadratický zbytek modulo } p \text{ a } a \not\equiv p \pmod{p} \\ -1 & \text{pokud a není kvadratický zbytek modulo } p \\ 0 & \text{pokud } a \equiv p \pmod{p} \end{cases}$$

Původní Legendreova definice byla pomocí explicitního výrazu.

Pro $p \in \mathbb{P} - \{2\}$ definujeme *Legendreův symbol* jako:

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \pmod p, \quad \left(\frac{x}{p}\right) \in \{-1, 0, 1\}.$$

Nyní si uvedeme několik vlastností Legendreova symbolu.

- Legendreův symbol je funkce periodický v prvním argumentu. Tedy platí:

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \quad \Leftrightarrow \quad a \equiv b \pmod p.$$

  Konkrétně budeme později potřebovat případ $\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right)$.

- Legendreův symbol je multiplikativní v prvním argumentu.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

- Ve speciálním případě $a = b$ máme.

$$\left(\frac{x^2}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{pro } p \nmid x \\ 0 & \text{pro } p \mid x \end{cases}$$

- Platí: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

4.3. Hilbertův symbol

Definice 20. Nechť máme pole F a nenulové prvky $a, b \in F$.

$$(a,b) = \begin{cases} 1 & \text{jestliže rovnice } ax^2 + by^2 = z^2 \text{ má netriviální řešení v } F \\ -1 & \text{jinak} \end{cases}$$

Hilbertův symbol počítaný v poli $\mathbb{Q}_p$ budeme zapisovat jako $(a,b)_p$.
Nyní si uvedeme některé vlastnosti hilbertova symbolu.

- $(a,b)_p = 1 \quad \Rightarrow \quad (aa', b)_p = (a,b)_p(a',b)_p$ pro $\forall a, a', b \in \mathbb{Q}_v^*$,
- $(a,-a)_p = 1 \quad \forall a \in F$,
  rovnice $ax^2 - ay^2 = z^2$ má řešení $x = y = 1, z = 0$ což není triviální řešení,
- $(a,b)_p = (a,-ab)_p \quad \forall a, b \in Q_v^*$ [?Wallenborn?] (str. 47-48).

Věta 8. Mějme $a, b \in \mathbb{Q}_v$, $p \in \mathbb{P}$ a zapíšeme $a = p^\alpha u$, $b = p^\beta w$, kde u, w jsou p-adické jednotky. Pak pro Hilbertův symbol platí:

$$(a,b)_p = \begin{cases} (-1)^{\epsilon(u)\epsilon(w)+\alpha\omega(w)+\beta\omega(u)} & \text{pro } p = 2 \\ (-1)^{\alpha\beta\epsilon(p)} \cdot \left(\frac{w}{p}\right)^\alpha \cdot \left(\frac{u}{p}\right)^\beta & \text{pro } p \neq 2 \end{cases}$$

kde $\left(\frac{w}{p}\right)$, $\left(\frac{u}{p}\right)$ jsou Legendreovy symboly, $\epsilon(u) = \frac{u-1}{2}$, $\omega(u) = \frac{u^2-1}{8}$

Důkaz. Důkaz je převzatý z [?Wallenborn?] (str.49-51). Některé potřebné věty jsou převzaty s odkazy přímo do [?Wallenborn?].
Čísla α, β má smysl brát pouze pro případ $\alpha, \beta \in \{0, 1\}$. Díky symetrii Hilbertova symbolu má pak smysl uvažovat jen čtyři případy.

1. Nejprve dokážeme vzorec pro případ $p \in \mathbb{P} - \{2\}$.

   (a) Případ $\alpha = 0, \beta = 0$. Pak $a = u, b = w$. Dosazením dostaneme $(a, b)_p = 1$. Musíme tedy ukázat, že pro u, v existuje netriviální řešení pro:

   $$ux^2 + wy^2 = z^2.$$

   Toto je kvadratická forma o 3 neznámých a podle [?Wallenborn?] (str 32) má netriviální řešení modulo p. Diskriminant této formy je roven $1uw$ což je součin p-adických jednotek, tedy je sám p-adickou jednotkou. Tedy má netriviální řešení.

   (b) Případ $\alpha = 1, \beta = 0$. Pak musíme zkontrolovat $(pu, w)_p = \left(\frac{w}{p}\right)$. Z předchozího kroku máme $(p, w)_p = 1$, tedy $(pu, w)_p = (u, w)_p (p, w)_p = (u, w)_p$.
   Kontrolujeme tedy platnost $(u, w)_p = \left(\frac{w}{p}\right)$. Pokud je w čtvercem modulo p, je rovnost splněna, jelikož budou obě strany rovny 1.
   Vezměme w které není čvercem modulo p. Předpokládejme, že máme netriviální řešení (x, y, z). Podle knihy [?Wallenborn?] (str. 48) můžeme předpokládat, že $y, z \in \mathbb{Z}_p^*$ a $x \in Z_p$. Pokud se na rovnici podíváme z pohledu $\mathbb{F}_p$ dostaneme $wy^2 = z^2$. Tedy w musí být čtvercem modulo p, což je v rozporu s předpokladem. Dostáváme tak $(p, w)_p = -1$.
   Díky symetrii Hilbertova symbolu máme tedy i případ $\alpha = 0, \beta = 1$.

   (c) Případ $\alpha = 1, \beta = 1$. $(pu, pw)_p = (pu, -p^2uw)_p = (pu, -uw)_p = \left(\frac{-uw}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{u}{p}\right)\left(\frac{w}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{u}{p}\right)\left(\frac{w}{p}\right)$. Což odpovídá vzorci.

2. Nyní vezmeme případ, kdy $p = 2$.

   (a) Případ $\alpha = 0, \beta = 0$. Musíme zkontrolovat, zda platí následující.

   $$(u, w)_2 = (-1)^{\epsilon(u)\epsilon(w) + 0\,\omega(w) + 0\,\omega(u)} = \begin{cases} 1 & u \equiv 1 (\text{mod } 4) \vee w \equiv 1 (\text{mod } 4) \\ -1 & \text{v ostatních případech} \end{cases}$$

   Připomeňme, že $2 \nmid u, w$.

   i. Případ $\alpha = 0, \beta = 0, u \equiv 1 \pmod 4$.
   V případě $u \equiv 1 \pmod 8$ máme dostáváme z věty Theorem 2.113 v [?Wallenborn?] (str. 44), že u je čtverec, tedy $(u, w_p) = 1$.
   V případě $u \equiv 5 \pmod 8$ znovu ze stejné věty dostáváme, že existuje z tak, že $z^2 = u + 4w$, tedy $(u, w_p) = 1$.

   ii. Případ $\alpha = 0, \beta = 0, u \equiv w \equiv 3 \pmod 4$.
   Pokud je x, y, z je řešením rovnice $uX^2 + wY^2 = Z^2$, musí platit $x^2 + y^2 + z^2 = 0 \pmod 4$. V $\mathbb{Z}/4\mathbb{Z}$ jsou čtverce pouze $0, 1$ tedy $x \equiv y \equiv z \equiv 0 \pmod 2$, což je triviální řešení. Tedy $(u, w)_p = -1$.

(b) Případ $\alpha = 1, \beta = 0$. Musíme zkontrolovat:

$$(2u, w)_p = (-1)^{\epsilon(u)\epsilon(w)+\omega(w)}.$$

Napřed dokážeme, že platí

$$(2, w)_p = (-1)^{\omega(w)}.$$

Jinými slovy:

$$(2, w)_p = 1 \quad \Leftrightarrow \quad w = \pm 1 \, (mod\, 8).$$

- ($\Rightarrow$) Existuje $x, y, z \in \mathbb{Z}_2$ takové, že splňuje

  $$2x^2 + wy^2 = z^2$$

  a $y, z \not\equiv 0 \pmod 2$. Tedy $y^2 \equiv z^2 \equiv 1 \pmod 8$. Můžeme tedy podmínku změnit na

  $$2x^2 + w = 1 \pmod 8.$$

  Modulo 8 jsou čtverce pouze $0, 1, 4$. Tedy $2x^2 \equiv 0$ nebo $2x^2 \equiv 2 \pmod 2$. Tedy $w = \pm 1 \pmod 8$.
- ($\Leftarrow$)
  i. ($w \equiv 1 \pmod 2$). w je druhá mocnina (mod 8) a tedy $(2, w)_v = 1$.
  ii. ($w \equiv -1 \pmod 2$). Rovnice

  $$Z^2 - 2X^2 - vY^2 \equiv 0 \pmod 8$$

  má řešení $(1, 1, 1)$. Tedy máme $(2, w)_v = 1$.

  Nyní ukážeme, že $(2u, w)_2 = (2, w)_2(u, v)_2$
  i. ($(2, w)_2 = 1$)) Pak $(2u, w)_2 = (u, w)_2 = (2u, w)_2(u, w)_2$.
  ii. ($(u, w)_2 = 1$)) Pak $(2u, w)_2 = (2, w)_2 = (2u, w)_2(u, w)_2$.
  iii. ($(2, w)_2 = (u, w)_2 = -1$) Jsme v případě, kdy máme

  $$w \equiv 3 \pmod 8 \quad \wedge \quad (u \equiv 3 \vee u \equiv -1 \pmod 8).$$

  Jelikož můžeme násobit w, u, jakýmikoli čtverci můžeme se dostat k následujícím případům:

  $$(u = -1 \wedge w = 3) \quad \vee \quad (u = 3 \wedge w = -5).$$

  Pak mají následující rovnice řešení (1,1,1)

  $$Z^2 + 2X^2 - 3Y^2 = 0 \qquad Z^2 - 6X^2 + 5Y^2 = 0.$$

  Tedy $(2u, w)_2 = 1$.

(c) Případ $\alpha = 1, \beta = 1$. Musíme zkontrolovat, že platí

$$(2u, 2w)_2 = (-1)^{\epsilon(u)\epsilon(w)+\omega(w)+\omega(u)}.$$

Vezmeme

$$(2u, 2w)_2 = (2u, -4uw)_2 = (2u, -uw)_2.$$

Máme tedy

$$(2u, 2w)_2 = (-1)^{\epsilon(u)\epsilon(w)+\omega(w)+\omega(u)} = (-1)^{\epsilon(u)\epsilon(-uw)+\omega(-uw)+\omega(u)}.$$

Máme $\epsilon(-1) = 1$, $\omega(-1) = 0$, $\epsilon(u)(1 + \epsilon(u)) = 0$. Dostáváme tedy

$$(2u, 2w)_2 = (-1)^{\epsilon(u)\epsilon(w)+\omega(w)+\omega(u)}.$$

□

4.4. Diskriminant

Definice 21. Mějme kvaternionovou algebru A na číselným polem F. Vezměme kvaternionovou algebru $A_v = A \otimes_F F_v$ nad F_v. Řekneme, že A je *rozvětvená* (*ramified*) ve v pokud A_v je algebra s dělením. V opačném případě řekneme, že se A štěpí ve v a platí $A_v \cong M_2(\mathbb{F}_v)$.

Definice 22. Mějme množinu všech v, kde je kvaternionová algebra A rozvětvená. Označme ji ji $Ram(A)$. *Diskriminant* definujeme jako

$$\Delta(A) = \prod_{v \in Ram(A)} v.$$

Věta 9. $A = \left(\frac{a,b}{F}\right) \cong \left(\frac{1,1}{F}\right) \cong M_2(F) \Leftrightarrow$ kvadratická forma $ax^2 + by^2 = 1$ má řešení v F.

Důkaz. Viz [?Maclach?] (str 87-88). □

Připomeňme, že $M_2(F)$ není algebra s dělením. Dostáváme tedy, že A je rozvětvená ve $v \Leftrightarrow (a,b)_v = 1$. Můžeme tedy pomocí Hilbertova symbolu počítat diskriminant kvaternionových algeber. Pro $(a,b)_v = -1$ se kvaternionová algebra $\left(\frac{a,b}{F}\right)$ štěpí ve v, tedy v bude jeden z prvočinitelů diskriminantu.

4.5. Výpočet diskriminantu na konkrétním příkladu

Věta 10. *Pro kvaternionové algebry* $A = (\frac{-1,b}{\mathbb{Q}}), b \in \mathbb{Z}$ *platí*

$$\Delta(A) = \begin{cases} 2 \cdot \Pi p_i & pro\ b = 4m+3 \vee b = 8o+6 \\ \Pi p_i & pro\ b = 4m+1 \vee b = 8o+2 \end{cases}$$

$$p_i \mid b, \quad p_i \in \mathbb{P}, \quad p_i = 4k+3, \quad k, m, o \in \mathbb{Z}.$$

Důkaz. Mějme kvaternionovou algebru $(\frac{-1,b}{\mathbb{Q}})$ a chceme spočítat její diskriminant.

1. Nejprve vezmeme $b = 2n+1$.

   (a) Vezmeme případ $p = 2$.
   $a = 2^0 \cdot (-1)$, pak $\alpha = 0$, $\epsilon(u) = \frac{-1-1}{2} = -1$,
   $b = 2^0 \cdot (2n+1)$, pak $\beta = 0$, $\epsilon(v) = \frac{2n+1-1}{2} = n$.

$$(-1,b)_2 = (-1)^{\epsilon(u)\epsilon(v)+\alpha w(v)+\beta w(u)} =$$

$$= (-1)^n = \begin{cases} -1 & \text{pro } n = 2m+1 \quad (b = 4m+3) \\ 1 & \text{pro } n = 2m \quad\ \ (b = 4m+1) \end{cases} m \in \mathbb{Z}$$

   Tedy algebra $(\frac{-1,b}{\mathbb{Q}})$ se štěpí ve 2 pro $b = 4m+3$, $\forall m \in \mathbb{Z}$.

(b) $p \nmid b \wedge\ p \neq 2$.
$a = p^0 \cdot (-1)$, $\alpha = 0$,
$b = p^0 \cdot (2n+1)$, $\beta = 0$.

$$(-1,b)_2 = (-1)^{\alpha\beta\epsilon(p)} \cdot \left(\frac{u}{p}\right)^{\alpha} \cdot \left(\frac{v}{p}\right)^{\beta}$$

$$(-1,b)_2 = (-1)^{0\cdot 0\cdot \epsilon(p)} \cdot \left(\frac{-1}{p}\right)^{0} \cdot \left(\frac{2n+1}{p}\right)^{0} = 1$$

Tedy algebra $(\frac{-1,b}{\mathbb{Q}})$ se neštěpí v $p \nmid b$.

(c) $p \mid b$.
$a = p^0 \cdot (-1)$, pak $\alpha = 0$,
$b = p^1 \cdot (\frac{2n+1}{p})$, $\beta = 1$.

$$(-1,b)_2 = (-1)^{\alpha\beta\epsilon(p)} \cdot \left(\frac{u}{p}\right)^{\alpha} \cdot \left(\frac{v}{p}\right)^{\beta}$$

$$(-1,b)_2 = (-1)^{0\cdot 1\cdot \epsilon(p)} \cdot \left(\frac{-1}{p}\right)^{1} \cdot \left(\frac{2n+1}{p}\right)^{0} = 1 \cdot (-1)^{\frac{p-1}{2}} \cdot 1 =$$

$$= (-1)^{\frac{p-1}{2}} = \begin{cases} -1 & \text{pro } p = 4k+3 \\ 1 & \text{pro } p = 4k+1 \end{cases} \forall k \in \mathbb{Z}$$

Tedy algebra $(\frac{-1,b}{Q})$ se štěpí v $p_i = 4k+3$, kde $k \in \mathbb{Z}$, p_i je prvočíslo, a $p_i \mid b$ pro $b = 2n+1$.

2. Nyní vezmeme $b = 4m+2$ (Případ $b = 4m$ nás nezajímá, jelokož b pak není square-free).

(a) $p = 2$.
$a = 2^0 \cdot (-1)$, pak $\alpha = 0$, $\quad \epsilon(u) = \frac{-1-1}{2} = -1$, $\quad w(u) = \frac{(-1)^2-1}{2} = 0$,
$b = 2^1 \cdot (2n+1)$, pak $\beta = 1$, $\quad \epsilon(v) = \frac{2n+1-1}{2} = n$.

$$(-1,b)_2 = (-1)^{\epsilon(u)\epsilon(v)+\alpha w(v)+\beta w(u)} = (-1)^{n} = (-1)^{-n+0\cdot w(v)+1\cdot 0} = (-1)^{n} =$$

$$= (-1)^{n} = \begin{cases} -1 & \text{pro } b = 8o+6 \\ 1 & \text{pro } b = 8o+2 \end{cases} \forall k \in \mathbb{Z}$$

Tedy algebra $(\frac{-1,b}{\mathbb{Q}})$, kde $b = 8o+6$ se štěpí ve 2 pro $o \in \mathbb{Z}$.

(b) $p \nmid b \wedge p \neq 2$.
a=p$^0 \cdot (-1)$, pak $\alpha = 0$, $\quad \epsilon(u) = \frac{-1-1}{2} = -1$, $\quad w(u) = \frac{(-1)^2-1}{2} = 0$,
$b = p^0 \cdot (4n+2)$, pak $\beta = 0$, $\quad \epsilon(v) = \frac{4n+2-1}{2}$.

$$(-1,b)_2 = (-1)^{0\cdot 1\cdot \epsilon(p)} \cdot \left(\frac{-1}{p}\right)^{0} \cdot \left(\frac{4n+2-1}{p}\right)^{0} = 1$$

Tedy algebra $(\frac{-1,b}{\mathbb{Q}})$ se neštěpí v $p \nmid b$.

(c) $p \mid b$.
$a = p^0 \cdot (-1)$, pak $\alpha = 0$,
$b = p^1 \cdot (\frac{2n+1}{p})$, pak $\beta = 1$.

$$(-1,b)_2 = (-1)^{\alpha\beta\epsilon(p)} \cdot \left(\frac{u}{p}\right)^{\alpha} \cdot \left(\frac{v}{p}\right)^{\beta}$$

$$(-1,b)_2 = (-1)^{0\cdot 1\cdot \epsilon(p)} \cdot \left(\frac{-1}{p}\right)^{1} \cdot \left(\frac{\frac{4n+2}{p}}{p}\right)^{0} = 1 \cdot (-1)^{\frac{p-1}{2}} \cdot 1 =$$

$$= (-1)^{\frac{p-1}{2}} = \begin{cases} -1 & \text{pro } p = 4k+3 \\ 1 & \text{pro } p = 4k+1 \end{cases} \forall k \in \mathbb{Z}$$

Tedy algebra $(\frac{-1,b}{Q})$ se štěpí v $p_i = 4k+3$, kde $k \in \mathbb{Z}$, p_i je prvočíslo, a $p_i \mid b$ pro $b = 4m+2$.

□

5. Závěr

V bakalářské práci jsme v první kapitole zavedli pojem kvaternionové algebry a některé jejich vlastnosti. Byly uvedeny příklady počítání s kvaternionovými algebrami a příklady důkazů isomorfismů mezi různými kvaterninovými algebrami.

V druhé kapitole jsme navázali pojmem řády kvaternionových algeber. Zabývali jsme se konkrétními příklady řádů a maximálních řádů. Vše jsme podpořili výpočty v programu SAGE.

V poslední kapitole jsme se zabývali diskriminantem algeber. Konkrétně jsme se zabývali výpočtem diskriminantu kvaternionových algeber $\left(\frac{-1,b}{\mathbb{Q}}\right)$.

Z kvaternionových algeber se využívají zejména Hamiltonovy kvaterniony pro rotace v trojrozměrném prostoru. Krom tohoto obecně známého využití jsou kvaternionové algebry spjaty s Kleinovými grupami které mohou být dále využity pro hyperbolické 3-variety. Zavedení aritmetiky v Kleinových grupách pomocí kvaternionových algeber vede k zajímavému propojení toerie čísel a goemetrie [?Maclach?].

Pokusili jsme se spočítat maximální řád přímým výpočtem, ale bohužel tento postup vede k soustavě rovnic o příliš mnoha neznámých. Pokud některé neznámé zvolíme pevně, dostaneme konkrétní řády, ale nemáme zajištěno, zda jsou maximální.

V této práci nebyl plně prostudován algoritmus SAGE pro počítání maximálních řádů kvaternionových algeber nad racionálními čísly. Není ověřeno, zda opravdu najde maximální řád ve všech případech. Touto tématikou lze navázat v dalších pracech.

Literatura

[1] MACLACHLAN, Colin a Alan W. REID. *The arithmetic of hyperbolic three-manifolds*. New York: Springer, c2003. ISBN 0387983864.

[2] MACÁLKOVÁ, Lenka. O kvaternionových algebrách. *Kvaternion* [online]. 2012, **2012**(2), 125–131 [cit. 2017-05-02]. ISSN 1805-1332. Dostupné z: http://kvaternion.fme.vutbr.cz/2012/kvat2_separaty/macalkova_sep.pdf

[3] MACÁLKOVÁ, Lenka. Kvaternionové algebry s programem SAGE. *Kvaternion* [online]. 2013, **2013**(1), 45–50 [cit. 2017-05-02]. ISSN 1805-1332. Dostupné z: http://kvaternion.fme.vutbr.cz/2013/kvat3_separaty/macalkova_final.pdf

[4] PRESZLER, Jason. *Introduction to p-adic numbers* [online]. University of Utah, 2005 [cit. 2017-04-30]. Dostupné z: http://www.math.utah.edu/ preszler/research/Qp.pdf

[5] WALLENBORN, Lars Ambrosius. *Computing the Hilbert symbol, quadratic form equivalence and integer factoring*. Bonn, 2013. Diplomová práce. Mathematisch-Naturwissenschaftlichen Fakultät der Rheinischen Friedrich-Wilhelms-Universität Bonn.

6. Seznam použitých zkratek a symbolů

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	přirozená, celá, racionální, reálná, komplexní čísla
F	vektorové pole, $char(F) \neq 2$
F^*	multiplikativní grupa nenulových prvků v F
$\overline{F}$	algebraický uzávěr F
$M_n(F)$	pole matic řádu n nad polem F
$Z(A)$	centrum algebry A
$\mathcal{H}$	Hamiltonovy kvaterniony
$v_p(n)$	p-adická valuace v n
$\left(\frac{x}{p}\right)$	Legendreův symbol
(a, b)	Hilbertův symbol
$V \otimes_F W$	tensorový součin vektorových prostorů V, W nad polem F